



**Models for Information Assurance Education and Outreach:
A Report on Year 2 Implementation***

Jianjun Wang

School of Social Sciences and Education

California State University, Bakersfield

September 15, 2014

* This program is funded by National Science Foundation under Grant No. DUE – 1241636.

Abstract

Models for Information Assurance Education and Outreach (MIAEO) is a NSF-funded, three-year project to support hands-on explorations in *network security* and *cryptography* through Research Experience Vitalizing Science -University Program (REVS-UP) at California State University, Bakersfield. In addition, the program incorporates components of curriculum development for undergraduate students and public forums for community members. During the second year of grant operation, MIAEO supported completion of five research projects in the *Information Assurance* domain. The hands-on exploration occurred during a four-week summer session and involved two professors, two university student assistants, two K-12 teachers, and 18 high school students. Besides evaluating the REVS-UP impact, this report includes assessment of compelling evidence in program development across the levels of *Intended Curriculum*, *Implemented Curriculum*, and *Attained Curriculum*. Feedback from the community outreach events has been gathered to show significant improvement of service outcome over last year. The report concludes with four recommendations to sustain the program effectiveness in the third year.

**Models for Information Assurance Education and Outreach:
A Report on Year 2 Implementation**

Table of Content

Abstract	2
Literature Review	5
Research Questions	8
Methods	9
Evaluation Findings	10
Recommendations	21
References	22
Appendix 1: Poster Presentations of Five IA Research Projects	24
Appendix 2: ISPS Speaker Event	30

Models for Information Assurance Education and Outreach:

A Report on Year 2 Implementation

Models for Information Assurance Education and Outreach (MIAEO) is a three-year project funded by NSF to enhance cybersecurity through research exploration, program development, and community outreach. Built on institutional resources at California State University, Bakersfield (CSUB), MIAEO incorporates three core components to articulate cybersecurity research in higher education:

- (1) Summer Bridge Investigation: A four-week Research Experience Vitalizing Sciences - University Program (REVS-UP) to involve high school students, K-12 teachers, and university student assistants in hands-on inquiry under the guidance of CSUB professors;
- (2) College Curriculum Development: A collaborative effort to strengthen multidisciplinary Information Assurance (IA) education for undergraduate students in Computer Science (CS) and Global Intelligence and National Security (GINS) programs;
- (3) Community Education Opportunity: Engagement of community partners to create a free course and a lecture series toward broad increase of IA literacy.

All three components have been launched since the program inception, which led to completion and dissemination of five research projects in the IA field last year:

- (1) Crack Me If You Can: Using GPU Machines to Crack Passwords
- (2) Defense Against Human Hacking
- (3) Zero Knowledge, We Know Everything ... !
- (4) Elliptic Enigma
- (5) Factor Fiction

(see Appendix 1 of Year 1 Evaluation Report at <http://www.csub.edu/~jwang/MIAEO1.pdf>)

Furthermore, outreach activities were extended to involve local high schools and communities during the first year of grant implementation:

MIAEO has invited 18 high school students, two K-12 teachers, and two CSUB student assistants to conduct research explorations in the fields of network security and cryptography. ... MIAEO faculty worked on curriculum developments in Information Assurance (IA) across multiple departments, and organized a public symposium to expand IA education for approximate 120 community members. (Wang, 2013, p. 2)

Stipulated by the original budget allocation for this NSF award (Grant No. DUE – 1241636), this report is prepared to evaluate MIAEO operation in the second year. Stufflebeam (2002) pointed out, “evaluation’s most important purpose is not to prove, but to improve” (p. 2). To address the dual emphases, this report not only includes a broad scope of evidence to assess the results-based accountability according to the original proposal, but also incorporates new recommendations to support program improvement toward the third year.

Literature Review

IA is an area of rapid development. Although Year 1 report included a review of research literature, more articles and reports have been disseminated in Academic Year (AY) 2013-14. Hence, a brief review of the new literature is needed to integrate the program evaluation with professional practice.

As an important funding source for IA capacity building, NSF renewed its call for proposals in 2014 to support “research on the teaching and learning of cybersecurity” through the CyberCorps(R): Scholarship for Service (SFS) program (NSF 14-586, ¶. 4). MIAEO was funded by the SFS program to maintain a close alignment with the national needs. In particular, *research, teaching, and learning* were highlighted as the key components for REVS-UP

activities. Gebauer (2014), the REVS-UP director across multiple disciplines, reconfirmed that “the program enables CSUB faculty to advance their research, and CSUB students get the opportunity to learn by teaching” (¶. 4).

Beyond the boundary of higher education, REVS-UP includes an outreach component to involve students and teachers from local high schools. Delker (2014) found that a properly designed summer program can “get more students interested in choosing computer science and cybersecurity as a career, leading them to get involved in computer security groups such as Capture the Flag and CyberPatriot in high school” (p. 1). Another research report also indicated the need to attract high school students in the field of science, technology, engineering, and mathematics (STEM) (Chen & Soldner, 2014). REVS-UP has been running at CSUB each summer since 2007 to support STEM education. The track record facilitated recruitment of quality students and teachers from high school to participate in cybersecurity investigations at CSUB.

As the only state university within a radius of two-hour driving, CSUB incorporates community services in its mission statement, i.e., “The University collaborates with partners in the community to increase the region's overall educational attainment, enhance its quality of life, and support its economic development.”^[1] In particular, community involvement is crucial in the IA field to reduce vulnerability of cyberspace infrastructure in this traditionally-underserved region. McDaniel (2013) concurred that “Partnerships with higher education institutions are essential because these institutions offer undergraduate and graduate programs that prepare graduates for positions in the government cybersecurity workforce and the private sector in support government cybersecurity goals” (p. 320). In MIAEO, the community need is addressed

[1] Source: http://www.csub.edu/about_csub/mission/

by a component of *College Curriculum Development* to strengthen IA education for undergraduate students in the local CS and GINS programs.

Bureau of Labor Statistics forecasted employment growth of 22% between 2010 and 2020 for information security analysts (Lockard & Wolf, 2012). Prior to the period of data projection, Chai (2009) noted that “there is a shortage of qualified personnel, which is a factor that contributes greatly to the society’s vulnerability to various cyber threats” (p. ix). Given the variation of cybersecurity issues, the original proposal of MIAEO suggested a multiple-disciplinary approach to fill a void in the existing IA degree programs:

Most information assurance degrees focus purely on the technical aspects of the field, neglecting criminal justice, political science, and intelligence skills. The proposed curriculum would combine the strengths of both existing programs [CS and GINS] to create well-rounded graduates with a broad base of knowledge. (see the MAIEO proposal: project summary)

The interdisciplinary root further strengthens program engagements with the general public, and thus, supports the community outreach component of MIAEO. In contrast, “the actual SFS solicitation requires only that an institution ‘provide clearly documented evidence of a strong existing academic program in cybersecurity’” (Hoffman & Torgas, 2014, p. 10). No interdisciplinary features were solely demanded in the NSF requirement, nor did the community outreach play a central role in the NSF announcement. In this regard, MIAEO remains an innovative feature in comparison to other projects in this field.

Meanwhile, the recent literature indicates a strong need for educating the public on importance of complying with applicable cyberspace safeguards in various fields (McDaniel, 2013). “With the amplified awareness of rising cyber security needs, universities are increasing

their curricula to include more cyber and security related courses to meet this intensified demand” (Souza, 2014, p. 28). Because “Institution outputs should be matched to employer needs” (Hoffman & Toregas, 2014, p. 4), the community engagement reciprocally enriches learning opportunities for college students to understand employment market in the local context.

By definition, “assessment” depicts a process of fact findings while “evaluation” includes more emphasis on the value judgment (Best & Kahn, 2005). In Year 1 report, the value of MIAEO was examined in a five-page section, “Creative Features of MIAEO” (see Wang, 2013, p. 5-9). New literature has been reviewed in this section to reconfirm the program value this year. As a result, a profound role has been identified for MIAEO to improve cybersecurity education on two fronts: (1) Enhancing the capacity of college-based learning through REVS-UP and IA program development, and (2) Increasing IA-literacy for the general public.

Research Questions

Hoffman and Toregas (2014) observed that “A previous report on SFS workforce development (Hoffman 2012) argued for a broader and more holistic approach to cybersecurity education” (p. 7). Led by university professors, a holistic approach has been taken in MIAEO to enrich learning and teaching opportunities at CSUB through collaborative efforts on cybersecurity research, curriculum development, and community outreach. To strengthen utility of this report, three research questions have been developed to guide data analyses for MIAEO evaluation:

1. Built on the REVS-UP platform from Year 1, what is the impact from research inquiries in the 2014 summer session?
2. What has been accomplished in curriculum development to enhance IA education?

3. What progress has been made to sustain the MIAEO commitment in community outreach?

These questions are important for multiple stakeholders. Within the local community, REVS-UP has become a high profile program for K-12 teachers and high school students. It attracted 365 student applicants last year, and the rate of acceptance was as low as 30%. Curriculum development and community outreach are critical because of their alignment with MIAEO's goal to "develop models for information assurance and outreach that can be implemented on a regional and national scale to increase interest in the field of information assurance and increase the capacity for high-quality education."^[1] Based on a premise that the whole could be larger than sum of its parts, analytic approaches are described in the method section to triangulate quantitative and qualitative findings for MIAEO evaluation.

Methods

Starting in 2013, NSF funding has provided additional support to offer opportunities of hands-on investigation in *network security* and *cryptography* for high school students, K-12 teachers, and CSUB student assistants. To address the result-based accountability, poster presentations are examined to illustrate completion of the research agenda led by two professors. Meanwhile, scholarly presentations and transcript records are analyzed to document subject competency of CSUB student assistants. School ratings are examined for high school students who participated in the REVS-UP exploration. Questionnaire feedback is gathered from K-12 teachers and high school students to cross-examine REVS-UP impact in the local context (Question 1).

The IA program development for CS and GINS majors is assessed according to well-

[1] p. 3 of <http://www.cs.csub.edu/~melissa/cv.pdf>

established curriculum theories. According to BEng (2010), curriculum development is categorized across multiple stages. At the first stage, Intended Curriculum (IC1) is considered in designing course syllabi. Based on IC1, Implemented Curriculum (IC2) is employed to describe what is taught in classrooms and mathematics/science labs. At the final stage, Attained Curriculum (AC) is examined to document student learning outcomes. This curriculum model was employed by the International Association for the Evaluation of Educational Achievement (IEA) in cross-national studies, such as the Third International Mathematics and Science Study (Plompp, 2014). In this report, it is adopted to examine what has been accomplished in program development for IA education (Question 2).

Document analyses are conducted to assess the impact of two events, (1) Information Security Professional Speakers in 2014 April, and (2) Dissemination workshop in 2014 August. Participant feedback is gathered to evaluate effectiveness of these events in community outreach and information dissemination (Question 3).

Findings

REVS-UP Outcomes

In the 2014 Summer session, two CSUB professors led a team of 18 high school students, two college student assistants, and two high school teachers to engage in hands-on exploration of IA research for four weeks. The team was divided evenly into two sections. Each section was brought together for about an hour in the morning to learn major security breaches from the past. Hands-on experiences were gained from the lab exploration during the remaining part of the day. This arrangement was designed to address the first recommendation of the last evaluation report, i.e., “Incorporate More Hands-on Activities” (Wang, 2013, p. 19).

Summary of Poster Presentations

The persistent effort in REVS-UP exploration has resulted in completion of five poster presentations to fulfill research agenda of the leading professors (see Appendix 1). A content analysis of the poster projects is summarized in Table 1.

Table 1: Content of Poster Presentations from REVS-UP

Project Title	Theme of Exploration
Network Scanning	Examine four programs, <i>Nmap</i> , <i>Snort</i> , <i>TCP Dump</i> , and <i>Wireshark</i> , to address network vulnerability issues.
Bitcoin and the SHA-256 Hashing Function	Explore pros and cons of Bitcoin, <i>a form of cryptocurrency</i> , and its related SHA-256 security system.
Integer Factorization Problem: An Attack on the RSA Public-Key Encryption Scheme	Employ Maple 16 to examine <i>Pollard's Rho Algorithm</i> and <i>Pollard's p-1 Factoring Algorithm</i> , both are better options than Trial Division that does not work well with semi primes.
How Secure is Your Password? GPU Password Cracking	Use multiple hash types, such as <i>MD5</i> , <i>SHA1</i> , <i>SHA256</i> , & <i>SHA512</i> , to calculate time differences across four categories (Dictionary Attack, Combo Attack, Word+Pattern Attach, and Pattern+Word Attack) for specific single-chip processors, i.e., GPUs-NVIDIA and GPUs-ATI/AMD.
Social Engineering: Hacking the Human Element	Treat human element as the weakest link in security protocols and apply Social Engineering tool to explore the methods of attackers through information gathering, communication modeling, pre-texting, and elicitation.

Accomplishments of CSUB Student Assistants

Without involvement of CSUB student assistants, one might wonder whether these topics were too complicated to engage high school students and K-12 teachers. Fortunately, the two student assistants have demonstrated strong subject competency to support the REVS-UP exploration. High school students reported,

Without Dr. Danforth and Alfonso Puga, the basic curriculum would have been painfully boring. Thankfully, they allowed me to branch out on my own for some additional research.

I loved the knowledge and expertise of Dr. Danforth and Alfonso Puga.

Alfonso Puga is a CSUB student assistant. He maintains a 3.22 GPA in *Computer Science*. His subject competency is illustrated by the following accomplishments this year:

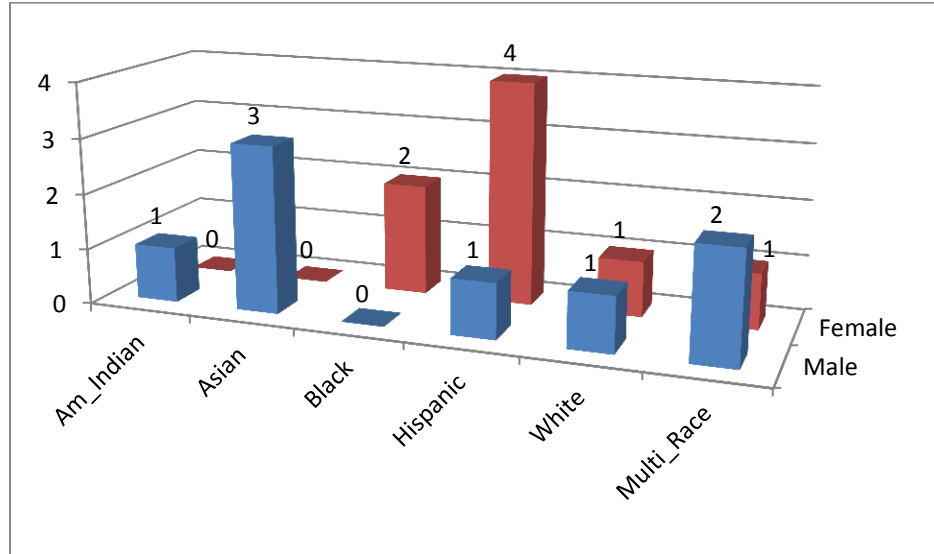
- (1) The first place recognition from a poster competition in the *computer sciences* category at the 2014 Emerging Researchers National Conference (<http://www.emerging-researchers.org/2014-2/>);
- (2) The first place in the *computer science and engineering* category of CSUB Student Research Competition;
- (3) Delivery of presentations at the CSU-wide Student Research Competition and the CSUB Student Research Poster Competition.

The other student assistant, Christian Elston, has a 3.92 GPA, and is recognized as the outstanding senior in *Computer Engineering* and the outstanding senior in *Natural Sciences, Mathematics, and Engineering*. Mr. Elston has been accepted by the master's program in *intelligence and national security* at Institute of World Politics. The establishment of subject competency has addressed the second recommendation of the last evaluation report, i.e., "Recruit Qualified Teaching Assistants" (Wang, 2013, p. 20).

Benefit to High School Students

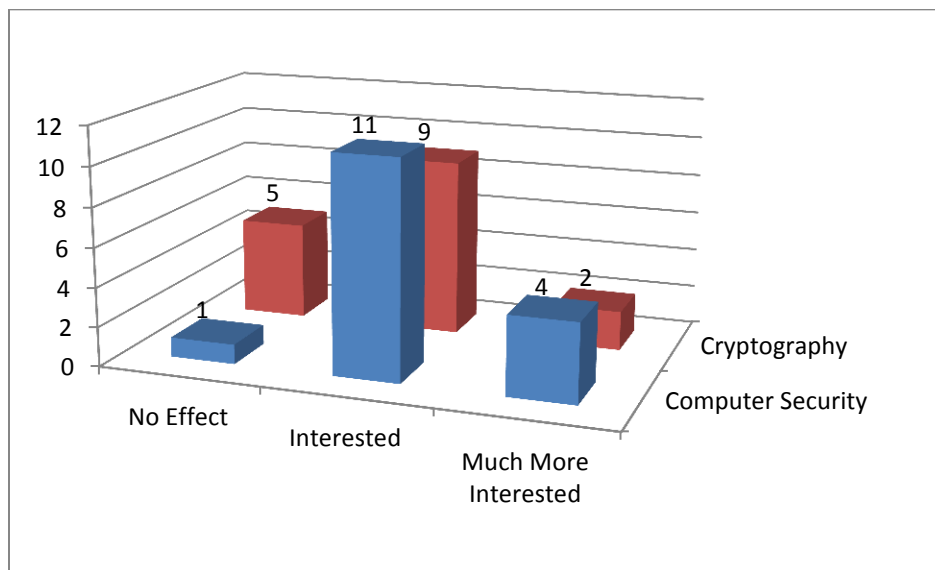
Although the majority of high school applicants were not accepted by REVS-UP, the stiff competition did not reduce diversity of high school students on demographic dimensions. Survey responses were gathered from 16 high school students who participated in the IA exploration sections. Figure 1 shows the student distribution across gender and ethnicity domains. The pattern indicates the project involvement of evenly-distributed male and female students from diversified ethnic backgrounds.

Figure 1: Gender and Ethnicity Distribution of High School Respondents



Students were asked to assess the impact of REVS-UP on their interest in *cryptography* and *computer security*. Figure 2 shows that REVS-UP has made the majority of high school students “interested” or “much more interested” in these fields.

Figure 2: Enhancement of Student Interest Through REVS-UP



Students were asked to confirm their agreement to a statement, “I am interested in computer security/cyber security.” The responses were categorized on a five-point Likert scale (1=“strongly disagree”, 5=“strongly agree”). With the intervention of REVS-UP investigation, the average rating increased from 3.81 to 3.88 between pretest and posttest.

The learning experience from REVS-UP is also linked to a change of student self-concept. Students indicated their agreement to the following statement, “I was prepared for this activity [hands-on REVS-UP exploration]”. The average response dropped from 3.69 in pretest to 3.63 in posttest on the Likert scale. Hence, the learning process seemed have made students more humble, which confirmed a well-known statement from Confucius, “The more a man learns, the more he knows his ignorance”.^[1]

The written feedback from students has been overwhelmingly positive in both pretest and posttest. Here is a sample of responses regarding student learning experiences:

I have experience with web development and very basic network security. I want to explore this field as a career option.

This activity interested me because it was something that I was looking to major in for college.

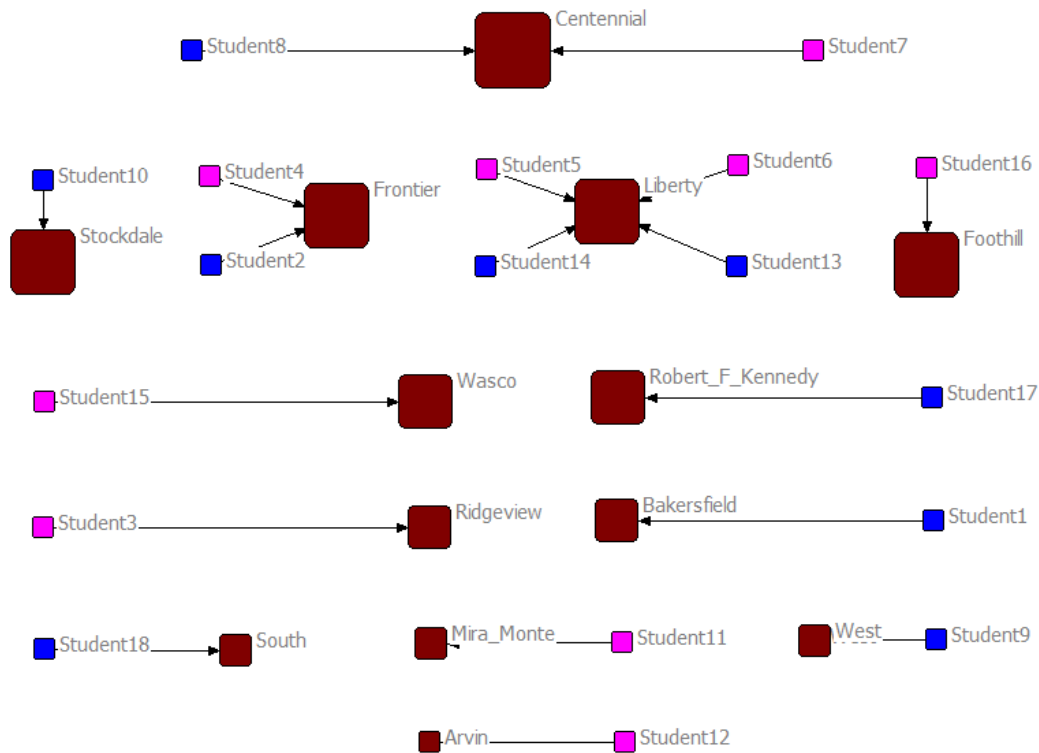
I liked the opportunity to work alongside other students of my age on a project. It allows me to learn something I otherwise wouldn't learn in my high school.

In addition to the individual learning outcomes, REVS-UP fosters development of student network across different high schools. Local schools are rated from 1(the worst) to 10 (the best) at greatschools.org according to student academic performance. A parent elaborated that “In my mind a 10 is excellent test scores across the board, a 5 is slightly below average and a 1 is a

[1] <http://novel.jschina.com.cn/yingyuwenxue/yinghmy/yinghanmingyan15.htm>

school where they shoot children for trying to use the library.”^[1] In general, it was reported that “GreatSchools is the leading source of information on school performance in the country”.^[2]

Figure 3: REVS-UP Student Network across Different Schools.



Legend: (1) Gender: pink – female, blue – male;

(2) School Rank: row 1 -> 9 (highest), row 2 -> 8, row 3 -> 7, row 4 -> 6, row 5 -> 5, row 6 -> 4 (lowest).

Figure 3 shows the opportunity of student collaboration across diversified schools. Due to the competition in REVS-UP application, half of the students came from schools at ranks 8 or 9. Nonetheless, the network in Figure 3 does include a quarter of the students from below-average schools on the last two rows. In addition, the student grouping is not systematically skewed toward male or female categories. The balanced network connections represent another benefit to support student involvement in the REVS-UP explorations.

[1], [2] <http://boards.straightdope.com/sdmb/showthread.php?t=675559>

Feedback from High School Teachers

Two high school teachers worked as team members during REVS-UP explorations. Although they are unlikely to switch careers to the cybersecurity field, REVS-UP has enriched their knowledge to impact student learning in high school. One teacher acknowledged that “I benefited professionally from this activity by securing private information and also encouraging students who are interested in computers to further their education in computer science.” The other teacher also related REVS-UP to high school classroom settings, and indicated that “it [REVS-UP] showed me some different ways to use math in my classroom as well as some real world connections for my students and the math they are doing in the classroom.”

After collaboration in the REVS-UP teams, both teachers expressed their satisfaction. One teacher reported,

I really would like to include a lesson on the history of and how a cypher works and are created. Also have the students try to break a simple cypher. This would be good for group building and problem solving skills.

The other teacher expected that “Students will learn how to create passwords that are unpredictable/guessable and we will crack codes and using the DNA model. Lesson plans [for future teaching] are still in the making.”

Both teachers commended the capacity of learning environment at CSUB. They indicated that “CSUB research environment is organized, up to date (new computers) and clean” and “CSUB research environment and staff is encouraging and self-motivated.” More importantly, they consistently rated CSUB faculty mentors and student assistants in a “very supportive” category. They also liked the involvement of high school students. One teacher indicated that “Working with the kids” was the part he liked most about REVS-UP. Another

teacher noted the entry-level engagement of REVS-UP, i.e., “This activity educated an individual who knew nothing about the internet.” Hence, REVS-UP not only offered group-based learning experiences, but also supported professional development for in-service teachers. As one teacher summarized, “This activity opened my eyes to awareness of the internet and information that can be hacked into by a number of tactics.”

In summary, MIAEO continues its summer-bridge program in information security through a stable REVS-UP platform. Like in Year 1, hands-on investigations have been led by two experienced professors and supported by two university student assistants. The education experiences are extended to two K-12 teachers and 18 high school students. Completion of professor research agenda is demonstrated by five research presentations in *network security* and *cryptography*. With more emphases on undergraduate research, student assistants have demonstrated their subject competency, completed bachelor degrees, and won several recognitions through result disseminations. As a result, the program operation in Year 2 has completely addressed two recommendations from Year 1 Evaluation Report (Wang, 2013).

College Curriculum Development

Two new factors are embedded in the curriculum development this year. One of them hinges on CSUB quarter-to-semester (Q2S) transition which requires an extensive review of all programs, including the ones that extend interdisciplinary supports for MIAEO. The other factor is reflected by personnel assignments. Professor Danforth, the MIAEO Director, has assumed the chair position in Department of Computer and Electrical Engineering and Computer Science (CEE/CS). The other professor, Dr. Charles Lam, has moved up to serve as the Interim Associate Dean at School of Natural Sciences, Mathematics, and Engineering (NSME). Both administrative responsibilities are time-consuming, particularly during the Q2S transition.

Despite the unexpected institutional changes, curriculum development has proceeded at a full speed to support a semester-based *Information Security* concentration. As was indicated in the program description, “The Information Security track is intended for students who wish to pursue a career in information assurance and security, either with government agencies or with industry.”^[1] Adjustments have been made at the Intended Curriculum (IC1) level to add two new core courses in computer science (ACM/IEEE CS2013) and scale back on the number of GINS courses to 4 to meet the upper-division course requirement.

In addition, program development has entered an Implemented Curriculum (IC2) stage, and *CMPS 445 Data Mining & Visualization* was taught in Winter 2014 to a class of 14 students. The class size is still considered healthy for a 400-level CMPS course in the undergraduate program. This class meets four days a week for both lecture and lab components to support *knowledge discovery in and visualization of* large datasets. Students are exposed to data mining concepts, information retrieval, analysis methods, storage systems (e.g., data warehouses and text-based information systems), visualization, implementation and applications.^[2] The first two lab assignments also include Ethics Across the Curriculum (EAC) components to enhance multidisciplinary approaches in student research.

Outcomes of the course offering are documented by student feedback to assess features of the Attained Curriculum (AC). Nine students provided responses, and eight of them would recommend this course. The AC analyses further identified needs for revising homework assignments and some laboratory assignments. Because Python did not work properly on the computer systems, a virtual machine with fully functioning software will be created for the next

[1] <http://www.cs.csub.edu/abet/semester/submitted/CMPS%20Catalog%20Copy%20-%20Track%20Changes%20version.docx>

[2] <http://www.cs.csub.edu/~melissa/courses.php?course=cs445&quarter=w14&category=info>

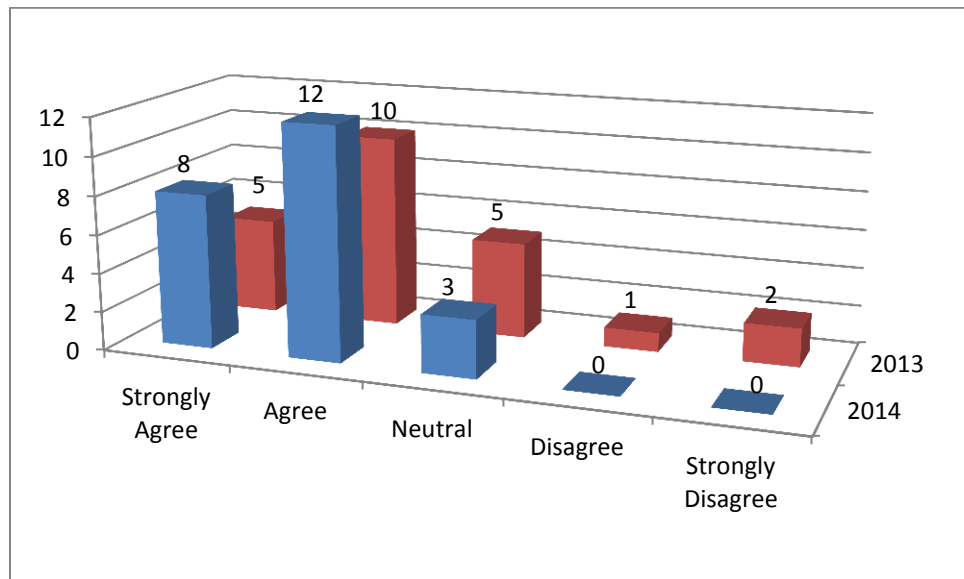
offering of this course.

In conclusion, MIAEO stays on a right track for curriculum development according to a thorough examination of the Intended Curriculum, Implemented Curriculum, and Attained Curriculum. Plans have been developed from the curriculum analyses to improve course assignments and virtual machine adoption for CMPS 445 in the future.

Community Education Events

The last recommendation from Year 1 Evaluation Report was on expanding community outreach approaches. In response, MIAEO hosted Information Security Professional Speakers (ISPS) on April 23, 2014 (Appendix 2) and sponsored a dissemination workshop on August 1, 2014. Similar to last year, attendee responses were gathered from the ISPS event. Most respondents “agreed” or “strongly agreed” that the presentation met their expectations.

Figure 4: Opinion on Whether This Presentation Met Attendee’s Expectation

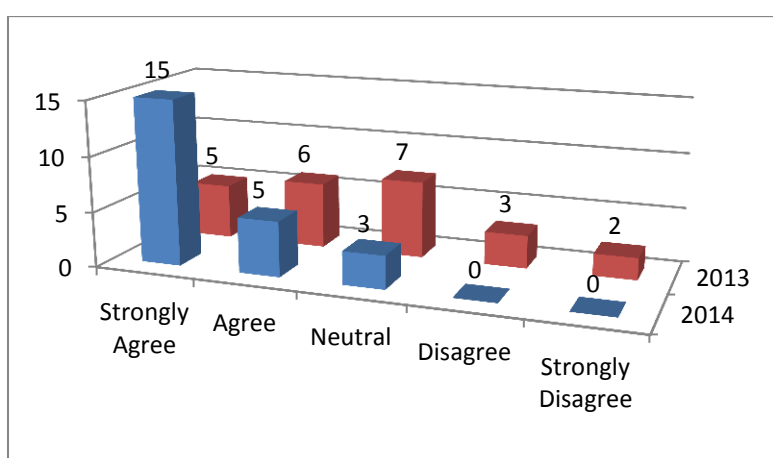


The Wilcoxon-Mann-Whitney test is employed to analyze the response difference between adjacent years. This non-parametric test is analog to the independent sample t test and

can be used when the response variable is measured on an ordinal scale. The result indicates significant improvement in attendee satisfaction over last year ($Z=1.69$, $p=.0454$).

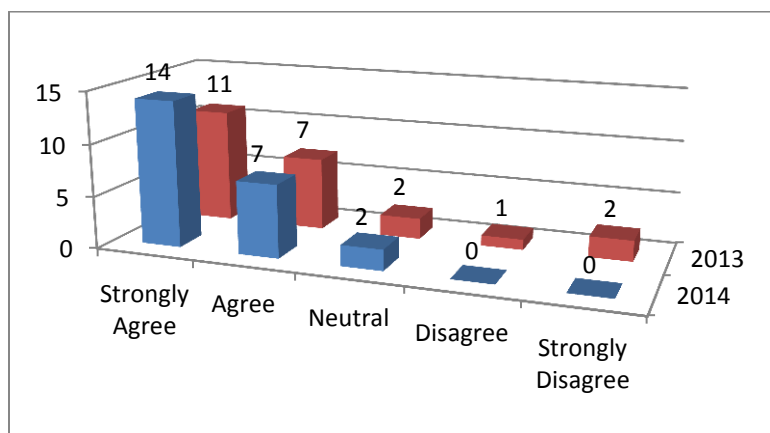
The ongoing improvement is also illustrated by attendee responses to another item on a Likert scale, “You learned helpful information at this event” (see Figure 5) The Wilcoxon-Mann-Whitney test reconfirms significant improvement in attendee opinions over last year ($Z=3.32$, $p=.0004$).

Figure 5: Acquisition of Helpful Information from ISPS



Survey responses in Figure 6 indicate that more attendees would attend similar events in the future, which supports sustainability of ISPS as an event of community interest.

Figure 6: Attendees Would Attend Similar Events in the Future



As a new component, the dissemination workshop was designed to distribute REVS-UP information to the general public. Twenty-two community members participated in this event. The MIAEO Director indicated that most attendees were K-12 teachers, an indispensable component for the REVS-UP team building.

In summary, MIAEO incorporated a dissemination workshop in its Year 2 operation. For the outreach effort through ISPS, the results demonstrated significant improvement of attendee satisfaction over last year. Accompanied with the other components of REVS-UP exploration and curriculum development, MIAEO has completely addressed all recommendation from the last evaluation report (Wang, 2013).

New Recommendations

At the time of awarding the MIAEO grant, the Q2S transition was not envisioned in the original proposal, nor did Professors Danforth and Lam expect to assume these major leadership positions in the CEE/CS Department and School of NSME. Despite these unexpected developments, MIAEO is running more smoothly than last year. One important factor is the maturity of student assistants to support MIAEO activities.

As both student assistants headed toward graduation this year, two new student assistants have been identified, one started working on research projects since 2014 May and the other joined the team this month. To sustain the program success, **the first recommendation is to enhance the mentorship for new student assistants in next year.**

The original faculty team for MIAEO includes three professors, Drs. Danforth, Lam, and Martinez. While this report covers *REVS-UP*, *Curriculum Development*, and *Community Outreach* components, the evaluator expects the latest update on a second *community outreach talk* and its associated evening course for community outreach. Hence, **the second**

recommendation is to expand the existing mechanism of data gathering to reflect effectiveness of these community outreach events.

ISPS has been offered twice in the first two years. Some presenters were commended highly by the attendees. For instance, multiple respondents praised a presenter named “Leif” or “Leaf”. Another respondent indicated that “It's all in the presenters. ... I as well as a few others got some tired eyes on the second presentation. Repetitious, monotone, standstill presenters are tough to hear.” To improve ISPS effectiveness, **the third recommendation is to enlarge the candidate pool for presenter selection and invite the ones who are experienced in public presentations.**

References

- BEng, C. (2010). *An investigation into the strategic application and acceleration of curriculum renewal in engineering education for sustainable development*. [Online] Retrieved from https://www120.secure.griffith.edu.au/rch/file/c723a9b3-8869-a011-c036-c80468264c1c/1/Desha_2010_02Thesis.pdf.
- Best, J. & Kahn, J. (2010). *Research in education* (10th ed.). New York: Pearson.
- Chai, S. (2009). *Three essays on behavioral aspects of information systems: Issues of information assurance and online privacy*. Buffalo, NY: University at Buffalo (UMI Number: 3356013).
- Chen, X. & Soldner, M. (2013). *STEM attrition: College students' paths into and out of STEM fields* (NCES 2014-001). Washington, DC: National Center for Education Statistics.
- Delker, K. (2014). *Hacking for a good cause: High schoolers learn the skills of the bad guys to fight cybercrime*. [Online] Retrieved from <http://news.unm.edu/news/hacking-for-a-good-cause>.
- Gebauer, A. (2014). *REVS-UP*. [Online] Retrieved from http://www.csub.edu/admissionsandaid/high_school_students/revs_up/
- Hoffman, L., & Torgas, C. (2014). *Whither SFS?: Cybersecurity SFS Workforce Development Workshop Report* (Report GW-CSPRI-2014-04). Washington, DC: The George Washington University.
- Lockard, C. & Wolf, M. (2012). *Occupational employment projections to 2020*. [Online] Retrieved from <http://www.bls.gov/opub/mlr/2012/01/art5full.pdf>.


- McDaniel, E. (2013). Securing the information and communications technology global supply chain from exploitation: Developing a strategy for education, training, and awareness. *Issues in Informing Science and Information Technology*, 10, 313-324.
- Plompp, T. (2014). *International assessments*. [Online] Retrieved from <http://education.stateuniversity.com/pages/2110/International-Assessments-INTERNATIONAL-ASSOCIATION-EVALUATION-EDUCATIONAL-ACHIEVEMENT.html>.
- Souza, C. (2014). *National cyber security: The responsibility of all sectors*. Utica, NY: Utica College (UMI Number: 1554448).
- Stufflebeam, D. (2002). *CIPP model checklist: A tool for applying the Fifth Installment of the CIPP Model to assess long-term enterprises*. [Online] Retrieved from <http://www.nylc.org/sites/nylc.org/files/files/250CIPP.pdf>
- Wang, J. (2013a). An assessment of education quality beyond dinner table discussions. *International Education Studies*, 6 (1), 111-116.

Appendix 1: Poster Presentations of Five IA Research Projects

1. Network Scanning

**Department
of CEE/
Computer
Science**

Network Scanning
 Beau Bikakis, Guang Jin Liu, Tue Le
Advisor: Dr. Melissa Danforth Assistant: Alfonso Puga



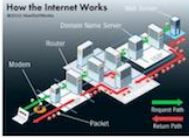
Background

How does the Internet work?

The Internet is the interaction of many connected devices across the world. It is a combination of hardware (computers, routers, servers, etc.) and protocols (a common set of rules for all internet devices to follow). All devices on the Internet can speak to each other because they all follow the same set of protocols (TCP/IP).

When a device is connected to the Internet through a local area network, it is given a special IP address to differentiate it from all the other devices that are also connected to the Internet. The IP address has two main functions: network identification and location addressing.

Client computers send requests to an Internet server in order to open web pages, watch videos, etc. The request goes through a series of routers to reach the Internet server, the server searches its database for data that matches the request and then sends back its response. The client is the input and the server is the output.




What is Network Scanning?

Network scanning is the use of scanning software to identify servers, devices, and clients on the network. It can be done by administrators looking to secure their network or hackers looking to exploit vulnerabilities.

How does Network Scanning work?


By using the correct programs and knowing how to use them, scanning networks can become quite easy. Those programs can scan network vulnerabilities, capture packets, and detect incoming threats. Keep this in mind when you are on the Internet as anyone can scan your web activity to quickly find unencrypted passwords and determine what websites you have been on.



Network Scanning Programs


Wireshark

- Scans network traffic.
- Analyzes packets (data that can be transferred over a network).
- Filters through packets to find specific criteria.
- Is graphics-based instead of terminal-based.
- Monitor data coming in and out of your network.



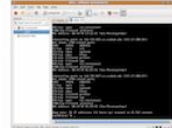
TCPdump

- Acts similar to Wireshark but has a different interface.
- Terminal-based.
- You type in command for which filter you want to apply.




Nmap

- Shows all hosts and devices connected to your network.
- Creates a virtual "map".
- Can determine the operating system of the target.
- Discovers hosts by sending a packet and analyzing the response.



Snort

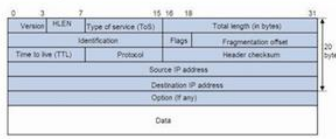
- Detect the intrusion of computers from outside world.
- Detect the intrusion in and out from the computer.
- Can choose between different types of alerts and actions for different inputs.
- Has three settings: sniffer, packet logger, and Network intrusion detection.



About the Network

Network

- Network is a subnet of links that get data to destination IP
- A Network is two or more computers linked together in order to share resources
- Data is organized into packets.
- There are series of headers for the different tasks within the packet.
- Host to network is physical connection between two machines, such as WiFi, Ethernet, etc.



Network Vulnerabilities

- Bugs in server programs, client programs, websites or web programs.
 - Mistake in program code.
 - Exploitable feature of program.
 - Malicious code.
- No default encryption that protects from packet sniffing.
- No verification of addresses and infrastructure servers.


Additional Info.

- Most programs shown here are totally free to download.
- It is illegal to scan other people's network without proper clearance.
- Permission is needed to scan other people's network.


References

- Wireshark: <http://www.wireshark.org/>
- TCPdump: <http://www.tcpdump.org/>
- Nmap: <http://nmap.org/>
- Snort: <https://www.snort.org/>
- IP protocol: <https://www.ietf.org/rfc/rfc791.txt>

2. Bitcoin and the SHA-256 Hashing Function





CSU Bakersfield
REVS UP
Research Experience Virtualizing Science University Program



bitcoin

And The SHA-256 Hashing Function

Taylor Redden, Chelsea Dalton, Jordan Lacava, Remy Verduzzo, Austin Burgeis
Advisor: Dr. Charles Lam Assistant: Frank Madrid

CSU Bakersfield
Research Experience Virtualizing Science University Program

What is Bitcoin?

Bitcoin is a form of cryptocurrency created in 2009 by an unknown person who went by the alias Satoshi Nakamoto. It is basically internet money, but instead of being controlled by an organization like Paypal, Bitcoin does not have any middlemen.^[1]

Obtaining a Bitcoin

Bitcoins may be obtained by buying, exchanging, selling, or earn them through mining. Mining is the process that allows for Bitcoins to be brought into the market, where they may then be sold. They can be purchased through Bitcoin ATMs or from other sellers.^[2]

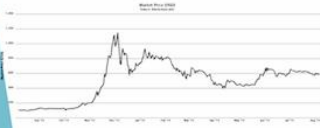
Bitcoin Benefits

- Mobile payments made easy
- Security and control over your money
- Works everywhere, anytime
- Fast international payments
- Zero or low fees
- Protect your identity^[3]

Bitcoin Drawbacks


- Securing your wallet
- Bitcoin price is volatile
- Bitcoin payments are irreversible
- Bitcoin is anonymous
- Instant transactions are less secure
- Bitcoin is still experimental
- Government taxes and regulations^[4]

Worth

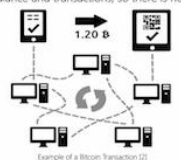


In the beginning, Bitcoin was only worth a few cents, but since then, it has peaked at \$1,200 and currently sits at about \$500.^[5]

Transactions



When you make a transaction, the data is sent to every node in the network where it updates the transaction tree, which basically verifies that you have enough Bitcoins to spend. Everyone can see everyone else's account balance and transactions, so there is no discrepancy with exchanges.




These transactions are then ordered in the block chain. Each of the blocks contains information on the inputs and outputs of a transaction and also the name of the previous block in order to link all the blocks. The blocks of the block chain are created through a process called mining.

Mining

Mining is used to expand the block chain as well as bring new Bitcoins to the market. When a user creates a new block, they receive a mining reward as well as any transaction fees. Anyone on the network can propose a new block, but it must meet special conditions. The SHA-256 hashing function is used to meet these conditions.

For better results, experienced miners invest in higher computing power found in more cutting-edge technology. But even with the most high tech gear, the competition is too stiff for any one person to profit from, so people join mining pools.^[6]



Into the SHA-256 Function

Bitcoin transactions are secured by SHA-256. This security system is used to encrypt transactions, addresses, wallets, etc, which allow the main user to be the only one that can read the information. SHA stands for "Secure Hash Algorithm" and the 256-bit model was created by the NSA to protect their information.^[7]

When you run the hashing function it will return a 64 character string. The hash for the word "hello" is:

```
2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1a742557304336293868824
```

Changing a single character in the original string will yield a completely different string. The hash for the word "jello" is:

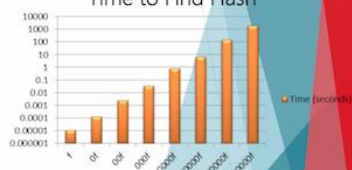
```
187c9bceeb919e1b3e6d20fa50ecab7d9d50b5343e88a3d912ac033929102e
```

To solve a block, the hash output needs to start with a certain number of zeros. The hash of the number "2036798186" is:

```
00000d624810aeb4aa6ed3e91290c25419391631e380a14461e8c204c86
```

To find this hash we pick random numbers until the hash is correct. Below shows the time it took to find a hash beginning with the specified number of zeros.

Time to Find Hash



Number of Zeros	Time (seconds)
1	~0.000001
2	~0.000002
3	~0.000004
4	~0.000008
5	~0.000016
6	~0.000032
7	~0.000064
8	~0.000128
9	~0.000256
10	~0.000512
11	~0.001024
12	~0.002048
13	~0.004096
14	~0.008192
15	~0.016384
16	~0.032768
17	~0.065536
18	~0.131072
19	~0.262144
20	~0.524288
21	~1.048576
22	~2.097152
23	~4.194304
24	~8.388608
25	~16.777216
26	~33.554432
27	~67.108864
28	~134.217728
29	~268.435456
30	~536.870912
31	~1073.741824
32	~2147.483648
33	~4294.967296
34	~8589.934592
35	~17179.869184
36	~34359.738368
37	~68719.476736
38	~137438.953472
39	~274877.906944
40	~549755.813888
41	~1099511.627776
42	~2199023.255552
43	~4398046.511104
44	~8796093.022208
45	~17592186.044416
46	~35184372.088832
47	~70368744.177664
48	~140737488.355328
49	~281474976.710656
50	~562949953.421312
51	~1125899906.842624
52	~2251799813.685248
53	~4503599627.370496
54	~9007199254.740992
55	~18014398509.481984
56	~36028797018.963968
57	~72057594037.927936
58	~144115188075.855872
59	~288230376151.711744
60	~576460752303.423488
61	~1152921504606.846976
62	~2305843009213.693952
63	~4611686018427.387904
64	~9223372036854.775808
65	~18446744073709.551616
66	~36893488147419.103232
67	~73786976294838.206464
68	~147573952589676.412928
69	~295147905179352.825856
70	~590295810358705.651712
71	~1180591620717411.303424
72	~2361183241434822.606848
73	~4722366482869645.213696
74	~9444732965739290.427392
75	~18889465931478580.854784
76	~37778931862957161.709568
77	~75557863725914323.419136
78	~151115727451828646.838272
79	~302231454903657293.676544
80	~604462909807314587.353088
81	~1208925819614629174.706176
82	~2417851639229258349.412352
83	~4835703278458516698.824704
84	~9671406556917033397.649408
85	~19342813113834066795.298816
86	~38685626227668133590.597632
87	~77371252455336267181.195264
88	~154742504910672534362.390528
89	~309485009821345068724.781056
90	~618970019642690137449.562112
91	~1237940039285380274899.124224
92	~2475880078570760549798.248448
93	~4951760157141521099596.496896
94	~9903520314283042199192.993792
95	~19807040628566084398385.987584
96	~39614081257132168796771.975168
97	~79228162514264337593543.950336
98	~158456325028528675187087.900672
99	~316912650057057350374174.801344
100	~633825300114114700748348.602688

Using the data we were able to create the formula: $\text{time} = 10^{(x-1)9994} \times 0.144$ (where x is the number of zeros). This can be used to find the time that it may take a computer to solve different hash functions. Using this formula, we predict that at 7 zeros, it takes about 33 minutes to find an appropriate answer. The current mining difficulty has 16 zeros. Based on this formula it would take our system about 210,000 years to find an answer.

[1] <http://regnews.com/what-is-bitcoin.html>
[2] <http://bitcoin.org/en/how-to-spend>
[3] <http://news.bitcoin.com/bitcoin-is-anonymous/>
[4] <http://www.bbc.com/news/technology-20140320-bitcoin-tax>
[5] <http://www.bloomberg.com/news/articles/2014-03-20-bitcoin-price-plunges-as-regulators-scrutinize>
[6] <http://www.bitcoinmagazine.com/tech/2014/03/20/bitcoin-mining-pools/>
[7] <http://www.fishbase.org/abstract.asp?id=10000>
[8] <http://www.fishbase.org/abstract.asp?id=10000>
[9] <http://www.fishbase.org/abstract.asp?id=10000>
[10] <http://www.fishbase.org/abstract.asp?id=10000>
[11] <http://www.fishbase.org/abstract.asp?id=10000>
[12] <http://www.fishbase.org/abstract.asp?id=10000>
[13] <http://www.fishbase.org/abstract.asp?id=10000>
[14] <http://www.fishbase.org/abstract.asp?id=10000>
[15] <http://www.fishbase.org/abstract.asp?id=10000>
[16] <http://www.fishbase.org/abstract.asp?id=10000>
[17] <http://www.fishbase.org/abstract.asp?id=10000>
[18] <http://www.fishbase.org/abstract.asp?id=10000>
[19] <http://www.fishbase.org/abstract.asp?id=10000>
[20] <http://www.fishbase.org/abstract.asp?id=10000>
[21] <http://www.fishbase.org/abstract.asp?id=10000>
[22] <http://www.fishbase.org/abstract.asp?id=10000>
[23] <http://www.fishbase.org/abstract.asp?id=10000>
[24] <http://www.fishbase.org/abstract.asp?id=10000>
[25] <http://www.fishbase.org/abstract.asp?id=10000>
[26] <http://www.fishbase.org/abstract.asp?id=10000>
[27] <http://www.fishbase.org/abstract.asp?id=10000>
[28] <http://www.fishbase.org/abstract.asp?id=10000>
[29] <http://www.fishbase.org/abstract.asp?id=10000>
[30] <http://www.fishbase.org/abstract.asp?id=10000>
[31] <http://www.fishbase.org/abstract.asp?id=10000>
[32] <http://www.fishbase.org/abstract.asp?id=10000>
[33] <http://www.fishbase.org/abstract.asp?id=10000>
[34] <http://www.fishbase.org/abstract.asp?id=10000>
[35] <http://www.fishbase.org/abstract.asp?id=10000>
[36] <http://www.fishbase.org/abstract.asp?id=10000>
[37] <http://www.fishbase.org/abstract.asp?id=10000>
[38] <http://www.fishbase.org/abstract.asp?id=10000>
[39] <http://www.fishbase.org/abstract.asp?id=10000>
[40] <http://www.fishbase.org/abstract.asp?id=10000>
[41] <http://www.fishbase.org/abstract.asp?id=10000>
[42] <http://www.fishbase.org/abstract.asp?id=10000>
[43] <http://www.fishbase.org/abstract.asp?id=10000>
[44] <http://www.fishbase.org/abstract.asp?id=10000>
[45] <http://www.fishbase.org/abstract.asp?id=10000>
[46] <http://www.fishbase.org/abstract.asp?id=10000>
[47] <http://www.fishbase.org/abstract.asp?id=10000>
[48] <http://www.fishbase.org/abstract.asp?id=10000>
[49] <http://www.fishbase.org/abstract.asp?id=10000>
[50] <http://www.fishbase.org/abstract.asp?id=10000>
[51] <http://www.fishbase.org/abstract.asp?id=10000>
[52] <http://www.fishbase.org/abstract.asp?id=10000>
[53] <http://www.fishbase.org/abstract.asp?id=10000>
[54] <http://www.fishbase.org/abstract.asp?id=10000>
[55] <http://www.fishbase.org/abstract.asp?id=10000>
[56] <http://www.fishbase.org/abstract.asp?id=10000>
[57] <http://www.fishbase.org/abstract.asp?id=10000>
[58] <http://www.fishbase.org/abstract.asp?id=10000>
[59] <http://www.fishbase.org/abstract.asp?id=10000>
[60] <http://www.fishbase.org/abstract.asp?id=10000>
[61] <http://www.fishbase.org/abstract.asp?id=10000>
[62] <http://www.fishbase.org/abstract.asp?id=10000>
[63] <http://www.fishbase.org/abstract.asp?id=10000>
[64] <http://www.fishbase.org/abstract.asp?id=10000>
[65] <http://www.fishbase.org/abstract.asp?id=10000>
[66] <http://www.fishbase.org/abstract.asp?id=10000>
[67] <http://www.fishbase.org/abstract.asp?id=10000>
[68] <http://www.fishbase.org/abstract.asp?id=10000>
[69] <http://www.fishbase.org/abstract.asp?id=10000>
[70] <http://www.fishbase.org/abstract.asp?id=10000>
[71] <http://www.fishbase.org/abstract.asp?id=10000>
[72] <http://www.fishbase.org/abstract.asp?id=10000>
[73] <http://www.fishbase.org/abstract.asp?id=10000>
[74] <http://www.fishbase.org/abstract.asp?id=10000>
[75] <http://www.fishbase.org/abstract.asp?id=10000>
[76] <http://www.fishbase.org/abstract.asp?id=10000>
[77] <http://www.fishbase.org/abstract.asp?id=10000>
[78] <http://www.fishbase.org/abstract.asp?id=10000>
[79] <http://www.fishbase.org/abstract.asp?id=10000>
[80] <http://www.fishbase.org/abstract.asp?id=10000>
[81] <http://www.fishbase.org/abstract.asp?id=10000>
[82] <http://www.fishbase.org/abstract.asp?id=10000>
[83] <http://www.fishbase.org/abstract.asp?id=10000>
[84] <http://www.fishbase.org/abstract.asp?id=10000>
[85] <http://www.fishbase.org/abstract.asp?id=10000>
[86] <http://www.fishbase.org/abstract.asp?id=10000>
[87] <http://www.fishbase.org/abstract.asp?id=10000>
[88] <http://www.fishbase.org/abstract.asp?id=10000>
[89] <http://www.fishbase.org/abstract.asp?id=10000>
[90] <http://www.fishbase.org/abstract.asp?id=10000>
[91] <http://www.fishbase.org/abstract.asp?id=10000>
[92] <http://www.fishbase.org/abstract.asp?id=10000>
[93] <http://www.fishbase.org/abstract.asp?id=10000>
[94] <http://www.fishbase.org/abstract.asp?id=10000>
[95] <http://www.fishbase.org/abstract.asp?id=10000>
[96] <http://www.fishbase.org/abstract.asp?id=10000>
[97] <http://www.fishbase.org/abstract.asp?id=10000>
[98] <http://www.fishbase.org/abstract.asp?id=10000>
[99] <http://www.fishbase.org/abstract.asp?id=10000>
[100] <http://www.fishbase.org/abstract.asp?id=10000>

3. Integer Factorization Problem: An Attack on the RSA Public-Key Encryption Scheme

Department
of
Mathematics

Integer Factorization Problem

An Attack on the RSA Public-Key Encryption Scheme

Maria Chumpitaz, Chad Cole, Haley Hamer, Alisa Iduma, Lucero Morales

Advisor: Dr. Charles Lam Assistant: Frank Madrid



Partial support for this work was provided by the National Science Foundation's Federal Cyber Service: Scholarship for Service (SFS) program under Award No. 1241636. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

Introduction:

RSA is one of the encryption systems that depend upon the complexity of the integer factorization problem to prevent an unwelcome third party from decoding the message. The function of this system involves a public key (n, e) , n being a product of two large prime numbers that are not easily factored and e being a random number between 1 and $\phi(n)$, and a private key (d) , which can be found using the formula: $e \cdot d \equiv 1 \pmod{\phi(n)}$. For example, Alice chooses a public and private key, then she makes the public key available to anyone who wants to send her a message. Once Alice gets an encrypted message back, only she is able to decrypt it with the private key. If the message is intercepted by an eavesdropper, he could possibly find the private key d by using the previous formula, then plug it into $c = m \cdot d \pmod{n}$, m being the decrypted message and c being the encrypted message.



Background:

Three possible ways to break the RSA algorithm are Trial Division, Pollard's Rho Algorithm, and Pollard's $p-1$ Factoring Algorithm. Trial division factors smaller numbers (less than one million) and does not work well with semi primes because they can be fairly large numbers. The Pollard Rho Algorithm allows the division process to be much quicker and allows the possibility of finding the two numbers that divide into a composite number. Pollard's $p-1$ Factoring Algorithm finds prime factors p by dealing with $p-1$. Each of the algorithms is efficient in certain cases.

Method & Data:

[†]The computer generates two random prime integers between the interval $2^{n-1} - 2^{n-2}$. Then the algorithm multiplies these two primes together to create n . Next, the algorithm tries to factor the n back into the two random primes p and q .

Trial Division

		Total Operations (100K runs)		
		Size(bits)	Time(s)	Time(per run(s))
1	<code>rand(1,rand(p,q))</code>	0	0.062	0.00062
2	<code>local: count=0</code>	0	0.327	0.00343
3	<code>for i from 1 to count(m,n) do</code>	2	1.591	0.015974
4	<code>count = count + 1</code>	3	3.385	0.033412
5	<code>if count = 1 then</code>	4	8.985	0.091666
6	<code> $ZZT[0] := "false";$ c := "count", count;</code>	5	20.217	0.2026574
7	<code> R;</code>	6	41.839	0.4184666
8	<code> if count[m] then</code>	7	89.030	0.89039
9	<code> $ZZT[0] := "true";$ count;</code>	8	182.022	1.8492022
10	<code> break;</code>	9	359.239	3.6948798
11	<code>end</code>	10	736.029	7.3739542
12	<code>if > 10 then</code>			
13	<code> generate := rand(2ⁿ - 2ⁿ⁻¹ + 1)</code>			
14	<code> n := count + 1</code>			
15	<code> for i from 1 to 1000 do</code>			
16	<code> n := nextprime(generate) + 1</code>			
17	<code> n := nextprime(generate) + 1</code>			
18	<code> draw(n) -> R;</code>			
19	<code> time() -> tE;</code>			

Trial division worked extremely fast for very small numbers. It depends on the factorization of the smallest primes, and it divides the number by the next prime until it works and is fully factored. According to the data gathered, the time grows exponentially as the bits increased. So with larger numbers, the time taken will increase greatly between two consecutive bits.

Pollard's Rho Algorithm

```

> function prc(p, q)
  local count, a, d;
  n ← p;
  count ← 0;
  count ← 2;
  b ← 2;
  while (true)
    count ← count + 1;
    a ← a2 + 1 mod n;
    b ← b2 + 1 mod n;
    d ← a2 - b2 + 1 mod n;
    d ← gcd(a - b, n);
    if d < n then
      RETURN("factor, d", "count", count);
    break;
  end if d < n then
    RETURN("fail", count);
  break;
end
end

> i ← 30;
  generate ramu(231 - 2i - 1 + 1);
  st ← time();
  for i from 1 to 1000 do
    p ← nextprime(generate());
    q ← nextprime(generate());
    rho(p, q);
  end for
  time(i) - st

```

In order to factor numbers, there are easier ways to factor than just dividing by the smaller prime numbers such as 2, 3, and 5 like trial division. Once the numbers begin to get larger, this becomes a lengthy and time consuming process. The Pollard Rho Algorithm allows the division process to be much quicker and allows the possibility of finding two numbers that can divide into the number. Based on the data obtained, the time increased as the numbers became larger. If one were to test further, one would expect the difference in time, between two consecutive numbers, to be even more drastic.

Pollard's p-1 Factoring Algorithm



```

1  procedure gen(p,q)
2    local n, a, b, m, c, d
3    n ← 1
4    a ← 1
5    m ← 3
6    while true do
7      while m < 10 do
8        m ← nextprime(m)
9      n ← floor(
10         (ln(n)) /
11         (ln(m)))
12      a ← power(p,m), n ← mod(a, c) mod n, c ← mod
13         (a, n)
14      if a = 0 then RETURN "Conver", B "Factor"
15      else B ← B + 1
16      if B > 10 then RETURN "Diver", B, n
17    end
18  end
19
20  i ← 0
21  generate ← random(2n - 2n-1 + 1)
22  for i from 1 to 1000 do
23    m ← nextprime(generate)
24    if m ≠ nextprime(generate) then
25      pow(p,q)
26    end
27  end
28  ctime ← t - st

```

	Number of Events	Time(s)	Time per event (s)
1	278	0.0001	0.00036
2	109	0.001	0.00918
3	110	0.00006	0.0006
4	263	0.00021	0.0008
5	234	0.00031	0.0013
6	315	0.00032	0.0012
7	229	0.00035	0.0015
8	500	0.00049	0.0024
9	842	0.00288	0.0034
10	1140	0.00394	0.0034
11	1638	0.01692	0.0103
12	1500	0.02081	0.0139
13	1148	0.03212	0.028
14	436	0.05388	0.0488
15	630	0.08062	0.0772
16	8173	0.136	0.166
17	15331	0.18244	0.12
18	27 035	0.28786	0.1065
19	39 662	0.38848	0.098
20	64117	0.50613	0.0774
21	77 662	0.78858	0.0642
22	106 549	1.11747	0.0533
23	154 335	1.56548	0.0431
24	208 379	2.14743	0.0359
25	266 966	3.4554	0.0283
26	440 126	6.319523	0.0143
27	597 200	8.61848	0.0144
28	806 127	12.72505	0.0157
29	1023 781	2.2304	0.0022
30	1416 253	5.1461	0.0036



Conclusion:

Trial division worked well for smaller numbers but became extremely time consuming for large numbers. Pollard's p-1 Factoring Algorithm was moderately better than trial division, however, as the numbers became even larger, it, too, took more time. Overall, Pollard's Rho Algorithm was the fastest and most effective method out of the three tested. Even though the algorithm was able to factor reasonably large numbers, there is a point where the value of n could become so large that no method could factor the number fast enough to crack the code for Eve before it becomes useless.

Future Work:

Aside from the algorithms researched in this project, there are many different methods that are more complex that can be used to solve the integer factorization problem. These include but are not limited to: elliptic curve factoring, random quadratic sieving, quadratic sieve, quadratic sieve number field sieve, factoring Random square factoring method finds the factors by finding the congruence of squared modulo of n , however, it has not been completely developed. The quadratic sieve factoring method is one of the fastest ways to factor and is similar to the random square factoring method except it requires large amounts of memory. The recommended size for RS is 4096-bits, basic unit of information, because it would be extremely expensive years to break. Therefore, people with adequate resources could further explore this method.


References:

1. Courtes, S. and Sankaranarayanan, A. "A Quick Tutorial on Pollard's Rho Algorithm". In: *Proc. of IEEE Conf. on Systems, Man, and Cybernetics*, 1991, pp. 100-103.
2. "Eavesdrop Stock Illustrations." *Eavesdrop Stock Illustrations*. N.p., n.d. Web. 04 Aug. 2014.
3. Menzies, A. J., Van Oorschot P. C., and Scott A. Vanstone. *Handbook of Applied Cryptology*. Boca Raton, CRC, 1997. Print.
4. "Pictures Of..." *A Young Boy Working On A Computer*. N.p., n.d. Web. 04 Aug. 2014.
5. "Record 232-digit Number from Cryptography Challenge Factored | Observations, Scientific American Blog." *Scientific American* Global RSS. N.p., n.d. Web. 04 Aug. 2014.
6. "RSA Key Sizes: 2048 or 4096 Bits?" *WiscKey*. N.p., 18 June 2013. Web. 05 Aug. 2014.
7. "Stock Photography and Stock Footage." *Clipart of Two Women Talking through Tin Cans* *JoeB071*. N.p., n.d. Web. 04 Aug. 2014.
8. "Incremental Data Mining." *Incremental Data Mining Using Multiplicities Monitors*. *Incrementando La Productividad*. N.p., n.d. Web. 06 Aug. 2014.

Performance at $\alpha = 0.100$ mm		
Issue (no)	Time (s)	Time per run(s)
0	0	0
1	124	00124
2	202	00202
3	260	00260
4	343	00343
5	468	00468
6	468	00468
7	1.185	01185
8	1.123	01123
9	1.170	01170
10	1.966	01966
11	4.353	04353
12	6.536	06536
13	6.927	06927
14	14.749	014749
15	21.495	021495
16	34.117	034117
17	50.361	050361
18	129.902	0129902
19	214.829	0214829
20	247.805	0247805

4. How Secure is Your Password? GPU Password Cracking

Department of CEE/ Computer Science



What are GPUs?
GPUs are single-chip processors primarily used to manage and/or provide the performance of video and graphics.

Why are GPUs used for cracking passwords?
GPUs are excellent at processing mathematical calculations and it has hundreds if not thousands of cores that can be used to compute multiple mathematical functions simultaneously. Basically, it is much faster to use a GPU for password cracking.

How password cracking works?
In our world of technology, there are two ways passwords are cracked. Either hackers try to crack your password by using simple logic or tools.

Methods:

Simple Logic	Tools
<ul style="list-style-type: none"> Name Combinations Hobbies Important Years/ Numbers 	<ul style="list-style-type: none"> Dictionaries Attacks Rules

Simple logic hackers, may be a close friend or an associate, use personal/public information already know about you to guess your password.
Dictionaries attacks scan through lists of preset words, phrases, and common passwords.
Brute-force attacks use every possible combination of letters, digits, and symbols to decrypt passwords.

Examples:

	Combinations	Possible Passwords
Password has 6 digits	$10 \times 10 \times 10 \times 10 \times 10 \times 10$	1,000,000
Password has 6 symbols	$32 \times 32 \times 32 \times 32 \times 32 \times 32$	1,073,741,824
Password has 6 letters (lowercase)	$26 \times 26 \times 26 \times 26 \times 26 \times 26$	308,915,776
Password has 6 characters (lowercase, uppercase, digits, & symbols)	$94 \times 94 \times 94 \times 94 \times 94 \times 94$	689,869,781,056

How Secure is your Password? GPU Password Cracking

Alwin Villamor, Cassandra Sanchez, & Ebony Turner
Advisor: Dr. Melissa Danforth Assistant: Alfonso Puga

Time Trials

	MD5	SHA1	SHA256	SHA512
Dictionary Attack (large.dict)	3 mins	5 mins	8 mins	35 mins
Combo Attack (large.dict/ common_passwords.dict)	3 days 10 hrs	7 days 4 hrs	15 days 3 hrs	42 mins
a 6 (Word+Pattern)	2 yrs 28 days	4 yrs 319 days	9 yrs 360 days	> 10 yrs
a 7 (Pattern+Word)	1 yr 347 days	4 yrs 359 days	> 10 yrs	> 10 yrs

Using the multiple hash types, such as: MD5, SHA1, SHA256, & SHA512, we calculated the times differences between attacks and GPUs- NVIDIA & ATI/AMD.

Attacks:

- a 0 (one dictionary attack)
- a 1 (two dictionary attacks)
- a 3 (brute force attack)
- a 6 (Word + Pattern attack)
- a 7 (Pattern + Word)

Rules:

- ?u : uppercase
- ?l : lowercase
- ?s : symbols
- ?d : digits
- ?a : all

Dictionaries:

- large.dict (7070 words)
- example.dict (129988 words)
- common_passwords.dict (3548 words)
- english_lower.dict (439833 words)
- combo2.dict (9025 words)
- combo3.dict (857375 words)

ATI/ AMD

	MD5	SHA1	SHA256	SHA512
Dictionary Attack (large.dict)	10 secs	16 secs	28 secs	39 secs
Combo Attack (large.dict/ common_passwords.dict)	41 mins	1 hr 39 mins	3 hrs 45 mins	11 hrs 42 mins
a 6 (Word+Pattern)	11 days 14 hrs	5 yrs 145 days 5 hrs	28 days 2 hrs	265 days
a 7 (Pattern+Word)	8 days 20 hrs	22 days 9 hrs	82 days 22 hrs	132 days

Tips

What makes a weak password?

- Is typically 8 characters or less
- Has common password patterns
- Is relevant to previous password
- Contains some public/ personal information about yourself

Ex. Special Dates
Names
etc.

What makes a strong password ?

- Is longer than 8 characters
- Has multiple characters and/ or difficult phrases
- Is (in no relation) connected to you personal or publicly

14 Passwords Decrypted

example.dict

- gnggo
- control
- 4man
- qandora
- kittykat
- password

large.dict

- nectarine
- kittykat
- bowlnoodle

combo3.dict/ example.dict

- 345qewrty
- qpplications

combo2.dict/ english_lower.dict

- qpplications
- qphatfood

english_lower.dict/ large.dict

- qpplications
- qphatfood

common_passwords.dict

- crashpanda

42 Total Passwords

- bowlnoodle
- crashpanda
- tw20nlyb_ts
- taxG@h164Z`yYmxF0
- qandora
- 4032h3110
- LagWWh@8jgk
- (jRla74Defm8j)
- X@ns790k
- G_O_g_0_7X
- whatIhad4BREAkFAST!
- V_ _Y7_@#
- @LLy`VnB43RBelong2US
- (7kaiPS`886
- 147HL25+M72jL
- highway123
- Help@World
- 345qewrty
- Help-Me
- YouKilledKenney
- tagM1B1Hh
- LoGpass775
- tw20nlyb_ts
- taxG@h164Z`yYmxF0
- 4032h3110
- LagWWh@8jgk
- (jRla74Defm8j)
- X@ns790k
- G_O_g_0_7X
- whatIhad4BREAkFAST!
- V_ _Y7_@#
- @LLy`VnB43RBelong2US
- (7kaiPS`886
- 147HL25+M72jL
- highway123
- Help@World
- 345qewrty
- Help-Me
- YouKilledKenney
- tagM1B1Hh

References

Hashcat: <http://hashcat.net/hashcat/>




GPU: http://en.wikipedia.org/wiki/Graphics_processing_unit

Password tips: <http://www.connectivity.org/tips-to-create-and-manage-strong-passwords/>

Methods for password cracking: <http://www.infosecisland.com/blogview/18538-Top-Ten-Password-Cracking-Methods.html>

Partial support for this work was provided by the National Science Foundation's Federal Cyber Service Scholarship for Service (FSSS) program under Award No. 1241638.

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.


Research Experience Visiting Science - University Program

5. Social Engineering: Hacking the Human Element

Department of CEE/Computer Science

Social Engineering: Hacking the Human Element

Mason Pawsey, Sonia Patino, Marissa Campos, Stephanie Acosta
 Advisor: Dr. Melissa Danforth Assistant: Alfonso Puga



Introduction

Today's companies must perform transactions and processes that involve handling data. That data can be company information, personal data, logistic information, etc. This information, if sold to the right person, can yield a massive profit for malicious agents. This provides motive for hackers to target the company. Hacking is the breaching of security to obtain information or some sort of good for personal gain. Companies are very aware of the problem that hacking poses, however, they often overlook a more simple approach for the hacker to compromise a company, social engineering.

What is social engineering?

THEY TAKE OUR SECURITY MEASURES AND TURN IT AGAINST US.

Social engineering is a tool widely used and often overlooked by companies. It exploits the weakest link in any security protocol, the human element. By preying on human nature, human tendencies, etc, hackers get useful personal/professional information that's then used to breach security.

Purpose

On a daily basis, thousands of attacks are launched against large and small companies to gather private and useful information of consumers around the world.

Our purpose is to explore the methods of attackers, to help protect private information and educate consumers like you and I.

Techniques

- Information Gathering
- Communication Modeling
- Pre-texting
- Elicitation

"Know thyself, know thy enemy. A thousand battles, a thousand victories."
 Sun Tzu

Information Gathering

Gathering information about your target is the most integral part of social engineering. Private information, public information, any kind of information is gathered to create a foundation for the social engineering engagement.

Communication Modeling

The way a social engineer communicates is vital to their information gathering. Gaining someone's trust depends on both their verbal and non verbal means, such as speech, tone of voice, body language, and touch. Because of the human nature, approaching someone in the right way will usually result in a polite and friendly encounter.

Berlos's SMCR Model of communication

Source	Encodes	Message	Channel	Decodes	Receiver
Communication Skills		Content	Hearing		Communication Skills
Attitudes		Elements	Seeing		Attitudes
Knowledge		Treatment	Touching		Knowledge
Social System		Structure	Smelling		Social System
Culture		Code	Tasting		Culture

Pre-texting

Pre-texting is a false motive that involves creating a new identity. Just like information gathering and communication modeling, pre-texting is a technique used by social engineers to persuade their target to release information or perform some action.

For example, a social engineer could pretend to be an employee of a big company and use the information gathering technique to compromise their security and possibly have physical access to their computers and networks.

Elicitation

This is a non-threatening, easy to disguise and effective technique that can be conducted in person, over the phone, or in writing. Elicitors may collect information about you or colleagues that could facilitate future targeting attempts. A trained elicitor exploits certain human or cultural predispositions. This includes: a tendency to answer truthfully when asked an "honest" question, a desire to be polite and helpful, a tendency to gossip, and a tendency to correct others.

Information Gathering

It would be in the company's best interest to train their employees and inform them of the techniques social engineers use.

Documents that contain personal information and company information should be disposed in a safe way, such as shredding and using secure disposal personnel to keep the information away from dumpster divers.

Communication Modeling/Pre-texting/Elicitation

Just because someone approaches you in a friendly way or looks the part does not mean that they are trustworthy. While it is not necessary to be cold and hostile towards those who try to strike up conversation, it's important to guard against possible infiltrations. You should not access your personal email through a company's network, and company information should be discussed with authorized personnel only.

It is best to know what information is NOT safe to give. Companies should inform their personnel of what information is acceptable to divulge.

91% of all passwords are one of the 1,000 most common

Conclusion

Companies spend outrageous amounts of money a year ensuring their security systems stay secure to protect their vendors and customers. Unfortunately, they often overlook the most important - and least secure - component of any system: the human element. Social engineering aims to exploit the lack of focus and diligence of employees with critical information that could lead to a breach in security. During our research, we explored the techniques and strategies used to compromise systems and what corporations can do to make sure their people and their sensitive data stays safe and secure.

How many of your passwords are based around YOUR personal information? Tip: Use upper/lower case letters, numbers and symbols to eliminate the chances of your password being guessed.

Acknowledgements

- Chevron
- National Science Foundation
- Cal State University of Bakersfield

Works Cited

Burnett, Mark. "10,000 Top Passwords." *Xato Passwords Security 10000 Top Passwords Comments*. Xato, 20 June 2011. Web. 04 Aug. 2014.

Hadnagy, Christopher. *Social Engineering: The Art of Human Hacking*. Indianapolis, IN: Wiley, 2011. Print.

Appendix 2: ISPS Speaker Event

“A Day in the Life of an Information Security Professional”

Speakers: Victoria Hurtado – Kern Health Systems
Leif Davisson – Kern Federal Credit Union

Victoria Hurtado grew up in San Jose, California. She received her Bachelor's in Business Administration and Marketing Management from California Polytechnic State University in San Luis Obispo and later received her Master's degree in Business Management from University of Phoenix. Victoria relocated to Bakersfield to join the KHS team in late 2011. Victoria is responsible for the Information Technology Operations at Kern Health Systems. Victoria provides technical leadership, vision, and day to day support for IT Operations. She is responsible for all of information systems and networking, security, and infrastructure within the organization. Although the main areas of discipline are infrastructure related, she plays an active role in Project Management, Technical Analytics, and Software Development. At KHS, they follow an Agile Methodology for software development lifecycle that is used to build workflows within the organization for process improvement.

Leif Davisson is a native of Bakersfield and has followed emerging technology throughout his career and work. Leif has worked as a Network Specialist at Kern Federal Credit Union since 2007. He fosters innovation and security awareness for staff and members. Prior to employment at Kern FCU Leif worked for the Kern County Treasurer and Sheriff's Department following his first job working at the CSUB ITA Staff Helpdesk. Leif earned his Degree in Business Administration (2010) with a focus in Management Information Systems. Leif continued his technical education and in 2012 passed both Network+ and Security+. Leif is an active member in the Kern Information Systems Security Association. In his spare time he enjoys membership in the Kern County Scottish and Irish Societies where he provides technical advice and enjoys others with similar interests.



Free Speaker Event

Wednesday April 23, 2014
BDC 402
3:30 – 4:30pm

Partial support for this event was provided by the National Science Foundation's Federal Cyber Service: Scholarship for Service (SFS) program under Award No. 1241636.

Any opinions, findings, and conclusions or recommendations expressed in this event are those of the speakers and do not necessarily reflect the views of the National Science Foundation.



CSU Bakersfield
 School of Natural Sciences,
 Mathematics, and Engineering